	Georgia Technology Authority		
Title:	**Data and Asset Categorization**		
PSG Number:	PS-08-012.01	**Topical Area:**	Security
Document Type:	Policy	**Pages:**	2
Issue Date:	3/20/08	**Effective Date:**	3/20/08
POC for Changes:	GTA Office of Information Security		
Synopsis:	Establishes a policy requirement to inventory and classify all state data and information processing systems throughout the enterprise.		

PURPOSE

Data is a critical asset of the State. All agencies have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the state, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form). However, to adequately protect the data, there must be an understanding of what to protect, why protect it and how to protect it. Data and asset classification is essential in this understanding and establishes the appropriate levels of protection and handling for the resources based on its value to the primary mission of the organization.

Security categories are based on the potential impact to an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

POLICY

Data Owner/s shall inventory and assign a security category to the data and the information processing systems, for which they hold responsibility. The security category assigned shall conform to FIPS 199 Standards for Security Categorization for Federal Information systems.

REFERENCES

- FIPS 199 at ***http://csrc.nist.gov***
- Georgia Digital Academy on Data Security (Appendices A and B) at ***http://gta.ga.gov***

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Data Categorization-Impact Level (Standard)
- Personal Information (Standard)

TERMS and DEFINITIONS

Security Categorization - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Objective – Confidentiality, Integrity, and Availability

- Confidentiality **-** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] (A loss of *confidentiality* is the unauthorized disclosure of information.)
- Integrity **-** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] (A loss of *integrity* is the unauthorized modification or destruction of information.)
- Availability **-** "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] (A loss of *availability* is the disruption of access to or use of information or an information system.)

Note: PSG number administratively changed from P-08-012.01 on September 1, 2008.